OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

09 JUL 1984

POLICY

MEMORANDUM FOR THE CHAIRMAN, DCI SECURITY COMMITTEE

SUBJECT: SECOM Long-range Plan Working Group

Reference is made to your memorandum, SECOM-D-013, of 18 January 1984, which established subject group to examine SECOM's role in the current environment; evaluate how well SECOM is fulfilling that role; review SECOM-monitored DCI security policies and procedures to assess their relevance and to determine the need to expand, contract or modify them; and, propose a broad program to guide SECOM activities for the next several years.

The Working Group has examined, reviewed and evaluated SECOM's role in today's world. In order to arrive at an assessment, we have considered the environment of the activity; the organizational setting, and the available assets. We have done this in the context of the perceived risk to the assets that we are obligated to protect in accordance with the SECOM mission, intelligence sources and methods. Our goal was not merely to correct any problems that we identified, or perceived, but to attempt to institutionalize, to some extent, the process of refining the SECOM's system of control over its activities.

We did not review SECOM-monitored DCI security policies and procedures to assess their relevance and to determine the need to expand, contract or modify them because it was concluded that such review is the mission of the various subcommittees and working groups of the SECOM, in the cases of specific disciplines, and the Committee as a whole in general mission fulfillment.

With this preface, the Long-range Plan Working Group submits the attached report, in the form of a series of recommendations, as proposals for your consideration.

Maynard C. Anderson
Director
Security Plans and Programs

R E P O R T

O F

THE DIRECTOR OF CENTRAL INTELLIGENCE SECURITY COMMITTEE

LONG-RANGE PLAN WORKING GROUP

Mr. Vernon E. Bishop, Department of State

Mr. Jerry Rubino, Department of Justice

[redacted] Central Intelligence Agency STAT

[redacted] National Security Agency STAT

Mr. Maynard Anderson, Department of Defense, Chairman

I. The SECOM needs to continue to seek greater uniformity of policies and procedures in order to ensure proper security with minimum costs.

II. The SECOM should aggressively pursue adequate funding for the performance of services of common concern to the Intelligence Community.

- Within the context of the SECOM, Members should assess their situations and arrive at an agenda for best achievement of common goals which they cannot attain on their own, such as training in specialized techniques.

III. There needs to be a broad analysis of personnel security without regard to previously imposed external or internal restrictions, with the objective of determining whether we are treating all facets of the discipline in the context of our times, e.g., the significance of certain aspects of an individual's life that have not been considered relevant such as:

- the fact of, or degree of religious commitment, if any;
- an individual's commitment to family life;
- community involvement, assumption of civic duties;
- type of avocations in which involved;
- engagement in activities directed toward self-improvement;
- the medical profile, to include psychological aspects.

(It is understood that because of political sensitivity, some of these considerations require judicious consideration. Further, the examples, and their relevance to adjudication, would mandate complete positive reporting of investigative results.)

IV. The SECOM should be a catalyst for personnel security research on a scientific basis; developments of requirements for behavioral science research that will better tell us what qualifications are necessary for Intelligence Community assignment and eligibility for SCI access, determine the personnel security requirements for determination of access (pre-indoctrination), for maintenance in status (supervisory security, etc.), and for post-debrief integrity (potential after actions), by:

- attempting to develop a psychological profile of an espionage agent (refer to FBI technique for profile development of criminal suspects on the basis of circumstance evaluations, etc.);

- case file study of failures (persons who did not succeed in maintaining responsibility for security of classified information) to include review of case files used in prosecution;

- examination of procedures to develop indicators of problems within our personnel (relationship of personnel management to personnel security);

- examination of pressures of society on custodians of classified information and the effects;

- on the basis of known activities, EEI, free-world estimates and evaluations, attempt to build an advanced "Red Agent" computer model to describe Soviet espionage behavior in the context of acquisition of Western classified information and, perhaps, eventually, sensitive technology. An advanced Red Agent could use state-of-the-art artificial intelligence techniques to produce a model able to reflect the best estimate and contrary view concepts of likely Soviet espionage behavior in future situations. Expansion, utilization and exploitation of such a model could assist in determining the most significant human vulnerability factors as well as those complementary investigative elements that must be stressed in order to properly determine the Subject's eligibility for access to classified information.

V. The SECOM should examine inconsistent personnel security practices by member agencies. The Working Group recognizes that a Working Group of the Personnel Security Subcommittee is preparing comments on this item, ad interim, however, it continues to believe that the issue must be emphasized as a long range objective and include the following considerations:

- improvement of the quality of personnel security investigations;

- preparation of a lexicon of standards for issuing non-SCI clearances among Intelligence Community organizations;

- examination of the results of the NSDD-84 study of personnel security in the Government vis-a-vis the Intelligence Community;

- distinctions among clearance requirements on the basis of depth of access, e.g., continuing access in depth vs. proximity, rather than merely the level of access;

- consistency of reinvestigation practices.

VI. The SECOM should continue to place additional and special emphasis on security awareness activities in order to:

- maintain a community data base of security education materials;

- improve threat briefs;

- improve counterintelligence awareness in industry.

VII. The SECOM should serve as the Intelligence Community "clearing house" for computer security issues.

- The SECOM should attempt to establish itself in a position of policy prominence in this area.

VIII. The SECOM should consider the establishment and operation of a Magnetic Media Destruction Center on behalf of U.S. Government agencies.

IX. If there is establishment of a community-wide leak data base concerning intelligence information, the SECOM should ensure continuing patterns and trends analysis.

X. The SECOM should examine its role in counter-terrorism and maintain cognizance of other Government efforts in this area by:

- monitoring appropriate activities dealing with counter-terrorism;

- evaluating security measures that can be taken or that are proposed for dealing with terrorism;

- evaluating intelligence reporting on terrorism as it pertains to the interests or concerns of the Members;

- coordination and analysis of available information that might be of assistance to Members.

XI. The SECOM should do a better job of promoting awareness of its successes and accomplishments by:

- providing its members a product that can be used to justify the contribution of resources by Departments and Agencies of the Intelligence Community such as an Annual Report which could include:

  - significant events of the past year

- highlights of particular importance
- subcommittee reports of events and activities of the past year
- the SECOM budget
- shortfalls in meeting the year's objectives, and
- objectives for the year ahead.

XII. The SECOM should continue its efforts to improve communications between and among its staff and its Members on matters of continuing interest by:

- reminding Members to maintain a close relationship with their subcommittee members to ensure continuing awareness of subcommittee activities;

- asking subcommittee chairmen to submit written monthly reports to the Chairman which can be disseminated to the Members prior to each meeting (with the agenda, perhaps) so that members can request discussion of any particular items of interest at the meeting and be prepared for such discussion;

- consider reformatting meetings to modify the structured subcommittee reports in favor of:

  - sharing of noteworthy membership experiences;
  - new business;
  - latest cases of interest (investigations, adjudications, etc.);
  - "theme" meetings in which one of the members would be responsible for developing a part of the program with a particular theme of general interest to the members;

- advising members of anticipated legislative requirements and initiatives.

XIII. The SECOM, as a whole, should reexamine its goals and objectives, principles and commitments, and standards of performance, following which there should be published clear guidelines for future performance.

XIV. The SECOM should hold formal sessions with subcommittee chairmen in order to identify the subcommittee's priority activities; to learn, in detail, all activities in progress; and, to give guidance and direction to the subcommittees. As a first step in the process, the Chairman should require each subcommittee chairman to submit goals and objectives for his group, specify how those will assist the SECOM in meeting its goals and objectives, and establish standards of performance for his group which will serve as the basis for evaluation of subcommittee success.

XV. The SECOM should establish a Subcommittee on the Future, which will evaluate security policies, procedures, techniques and implementation in the context of the anticipated, albeit uncertain environments, to include the implications of modern morality and emerging technology, in which we will be required to protect sensitive information.